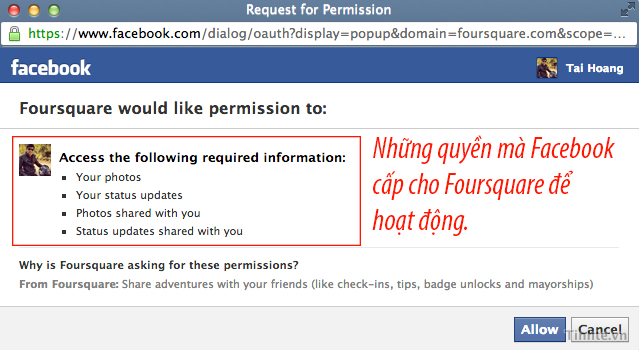
 ​

[OAuth](http://www.tinhte.vn/tags/oauth/) rất hay, nếu bạn thấy một website (hay phần mềm) nào đó cho phép [đăng nhập](http://www.tinhte.vn/tags/%C4%91%C4%83ng+nh%E1%BA%ADp/) bằng [tài khoản Facebook](http://www.tinhte.vn/tags/t%C3%A0i+kho%E1%BA%A3n+facebook/) hay [Google](http://www.tinhte.vn/tags/google/) mà không cần tạo nick mới thì rất có khả năng đó chính là OAuth. Đây là một chuẩn xác thực mở được rất nhiều các website và phần mềm sử dụng. Câu hỏi đặt ra là: Sử dụng OAuth có an toàn hay không? Tài khoản [Facebook](http://www.tinhte.vn/tags/facebook/) với Google có dễ bị hack nếu dùng OAuth hay không? Câu trả lời là OAuth rất an toàn, nó an toàn hơn cả việc bạn tạo một nick mới để đăng nhập một website.  
  
**Ưu điểm:**  
- Tiện lợi, nhanh chóng: không cần phải tạo nick mới mỗi khi đăng nhập vào một website hay phần mềm.  
- An toàn: Hạn chế được tình trạng đánh cắp mật khẩu, thông tin cá nhân.  
  
**OAuth không phải là OpenID**  
OpenID cũng là một dạng xác thực danh tính dùng nick từ tài khoản xxx để đăng nhập vào trang yyy. Về nguyên tắc thì hai loại này giống nhau nhưng cách hoạt động của chúng thì lại khác nhau. OpenID đòi hỏi người dùng phải cung cấp thông tin cá nhân còn OAuth thì không.  
  
**Ví dụ về OAuth**  
Ví dụ về phần mềm Foursquare trên điện thoại, khi lần đầu mở Foursquare lên, bên cạnh việc tạo nick mới, phần mềm này sẽ cho phép bạn đăng nhập bằng tài khoản Facebook. Bạn có thể đăng nhập theo cách này mà không cần phải tạo tài khoản mới hay nhập lại thông tin đăng nhập của mình. Đó chính là bạn đang sử dụng OAuth. So với cách tạo nick mới rồi đăng nhập thì OAuth an toàn hơn vì nếu lỡ Foursquare bị hacker tấn công thì thông tin của bạn sẽ không bị đánh cắp, tài khoản Facebook cũng được an toàn.  
  
Nếu bạn làm theo cách cũ, tức là đăng ký nick Foursuqare mới rồi đăng nhập, tức là Foursquare sẽ lưu trữ tất cả thông tin cá nhân của bạn, trong đó quan trọng nhất là email (Username) và mật khẩu. Foursquare bị hack đồng nghĩa với việc các thông tin này cũng rơi vào tay hacker. Còn khi dùng OAuth thì Foursquare sẽ không có được các thông tin cá nhân trên. Khi bạn đăng nhập bằng tài khoản Facebook thì cái mà Foursquare nhận được từ Facebook chỉ là một cái chìa khóa (token) chứa một số quyền hạn nhất định (không bao gồm quyền truy cập đến thông tin Username và Password). Cho nên nếu bị tấn công thì hacker chỉ lấy được những chìa khóa gần như vô dụng trên, còn Username và Password thì vẫn an toàn.

 ​

**OAuth hoạt động như thế nào?**  
Khi bạn đăng nhập bằng Facebook, Foursquare sẽ dẫn bạn đến trang (hoặc phần mềm) Facebook và liệt kê những quyền mà nó cần phải có để cho phép bạn đăng nhập và sử dụng dịch vụ. Nếu bạn đồng ý thì lúc này Facebook sẽ phát cho Foursquare một cái chìa khóa. Bên trong chìa khóa này chứa một số quyền hạn nhất định giúp cho Foursquare có thể xác minh bạn là ai cũng như giúp cho Foursquare có thể hoạt động được. Bạn cứ tưởng tượng chìa khóa này giống như chìa khóa mỗi phòng trong nhà của bạn. Nhà bạn có nhiều phòng, khi khách (Foursquare) đến thì chủ nhà chỉ phát cho khách một chiếc chìa khóa duy nhất để mở đúng một phòng nhất định, còn các phòng chứa thông tin khác thì vẫn khóa, Foursquare không có quyền truy cập vào đó. Giả sử trên đường Foursquare bị cướp (hacker) tấn công, lấy mất chìa khóa vào phòng thì bọn cướp cũng chỉ mở được có một phòng duy nhất mà thôi (bên trong chứa các quyền để Foursquare có thể hoạt động được). Do đó cách đăng nhập bằng phương thức OAuth này rất an toàn cho người dùng cuối như chúng ta.  
  
Nếu bạn đăng nhập bằng tài khoản Google khác hay [Twitter](http://www.tinhte.vn/tags/twitter/) thì cũng tương tự. Nhiều bạn sẽ băn khoăn liệu đăng nhập bằng tài khoản Facebook hay Google như thế thì tài khoản Facebook/Google có an toàn không. Câu trả lời là an toàn bạn nhé. Nhắc lại là Facebook chỉ phát chìa khóa chứa một số quyền hạn nhất định, hacker có lấy được chìa khóa này từ Foursquare thì tài khoản Facebook cũng không bị mất mát gì đâu. Tuy nhiên lúc này bạn nên vào trang cài đặt của Facebook và xóa bỏ chìa khóa đó, mục đích là để xóa sổ những quyền hạn đã cấp vì hacker có thể dùng các token này để spam trên trang Facebook của bạn.  
  
**Vậy chúng ta có nên sử dụng OAuth không?**  
Câu trả lời là nên, và nó cũng rất dễ quản lý. Nếu website đó bị hack thì bạn chỉ cần vào lại Twitter hay Facebook rồi gỡ bỏ quyền truy cập của website đó là xong, giống như việc bạn thay đổi chìa khóa phòng vậy, token đã cấp trước kia sẽ không còn sử dụng được nữa và bạn cũng không bị mất mát thông tin gì.